ON A CLASS OF ARITHMETIC FUNCTIONS SATISFYING
A CONGRUENCE PROPERTY

J. Fabrykowski* and M. V. Subbarao**

I. INTRODUCTION AND PRELIMINARIES

A real or complex valued arithmetic function \( f(n) \) is said to be multiplicative whenever the relation \( f(ab) = f(a)f(b) \) holds for relatively prime integers \( a \) and \( b \).

In 1966 Subbarao [7] proved that if \( f(n) \) is multiplicative, integer-valued arithmetic function satisfying

\[
f(n+k) = f(n) \pmod{k}
\]

for all positive integers \( n \) and \( k \), then either \( f(n) = 0 \) or \( f(n) = n^r \) for a nonnegative integer \( r \). He also remarked that it is enough to take \( k \)'s as power of primes. Later Somayajulu [6] proved the same, taking \( k \)'s as primes but replacing the multiplicativity of \( f(n) \) by a stronger property. In 1955 de Bruijn [1] showed that an integer-valued arithmetic function satisfies (1.1) for all integers \( n > 0, k > 0 \) if and only if it can be written in the form \( f(n) = \sum_{i=0}^{\infty} c_i A(i) \left( \frac{n-1}{i} \right) \), where \( c_i \) are integers and \( A(i) = \text{l.c.m.} (1, 2, \ldots, i) \). His result was generalised by Carlitz [2]. It is clear that every polynomial with integer coefficients satisfies (1.1) but if \( f(n) \) is not a polynomial then Ruzsa [5] obtained that

\[
\lim_{n \to \infty} \frac{\log |f(n)|}{\log n} = \infty \text{ and } \limsup_{n \to \infty} \frac{\log |f(n)|}{n} > \log (e-1).
\]

In the present paper we generalize the result of Subbarao [7]. For this purpose, we introduce a certain class of arithmetic functions, called quasi-multiplicative functions—which includes the class of multiplicative functions on a proper subclass.

* Supported by NSERC Grant \#A-3062.
** Supported by part by NSERC Grant \#A-3103.

1980 Mathematics Subject Classification: 10A20.
A positive integer \( m \) is said to be squarefull (or powerfull) if for every prime \( p \mid m \) also \( p^a \mid m \) with \( a > 2 \). Using the convention that unity is both squarefree and squarefull we see that every positive integer \( n \) can be expressed uniquely as

\[
(1.2) \quad n = n_1 n_2, \quad (n_1, n_2) = 1
\]

where \( n_1 \) and \( n_2 \) are respectively squareful and squarefree integers.

1.3. Definition. An arithmetic function \( f(n) \) is said to be quasi-multiplicative whenever for every positive integer \( n \) we have

\[
(1.4) \quad f(n) = f(n_1) \prod_{p \mid n_2} f(p),
\]

where \( n_1 \) and \( n_2 \) have the meaning as in (1.2) and \( p \)'s are prime divisors of \( n_2 \).

It is easy to see that every multiplicative function is also quasi-multiplicative but not conversely, as the following example shows:

let

\[
f(n) = \begin{cases} 
1 & \text{if } n = 1, \rho \text{ or } \rho^2 \\
1 & \text{if } n = n_2 \rho^a, n_2 \text{-squarefree } (n_2, \rho) = 1, a > 0 \\
2 & \text{otherwise.}
\end{cases}
\]

Next, we note that from Definition 1.3 we have the following:

1.5. Theorem. An arithmetic function \( f(n) \) is quasi-multiplicative if and only if for every integer \( m \) and prime \( p \) such that \( p \mid m \) or \( p = 1 \) we have:

\[
(1.6) \quad f(mp) = f(m) f(p).
\]

The proof is easy and is omitted. We may use (1.6) as an alternative definition of a quasi-multiplicative function.

2. THE THEOREM

We shall prove the following main result.

2.1. Theorem. Let \( f(n) \) be a quasi-multiplicative integer-valued function satisfying

\[
(2.2) \quad f(n + p) = f(n) \pmod{p}
\]
for all positive integers \( n \) and all primes \( p \). Then either \( f(n) = 0 \) or \( f(n) = n^r \) for a non-negative integer \( r \).

2.3. *Remark.* Theorem 2.1 fails to be true if we assume that the congruence (2.2) holds only for a finite set of primes. To show this, let \( \beta = \{p_1, p_2, \ldots, p_k\} \) be any finite set of primes \( p_i \). Let \( \lambda = \left( \prod_{i=1}^{k} p_i \right) + 1 \).

Take the multiplicative function \( f(n) \) defined by: \( f(1) = 1 \),

\[
f(p^a) = \begin{cases} 
\lambda^a & \text{if } p \in \beta \\
1 & \text{if } p \notin \beta
\end{cases}
\]

so, if \( n = \prod_{p \in \beta} p^\alpha q^\beta \) then, since \( f \) is multiplicative \( f(n) = \lambda^{\omega(n_1)} \), where \( n_1 = \prod_{p \in \beta} p^\alpha \) and \( \omega(n_1) \) denote the number of distinct prime factors of \( n_1 \). We see that the values of \( f(n) \) are either 1 or \( \lambda^a \) for some positive integer \( a \). Therefore (2.2) holds every \( n \) and \( p \in \beta \) but \( f(n) \neq n^r \). This example shows how to construct infinitely many other functions with this property, since for \( \lambda \) one could take any polynomial of \( \prod_{i=1}^{k} p_i \) with integer coefficients and constant term 1.

In order to prove the Theorem we need the following result due to Polya [4]:

2.4. *Lemma.* If \( f(x) \) is quadratic polynomial in \( x \) with integer coefficient such that \( f(x) \neq a(bx + c)^2 \) and if \( p_n \) denote the greatest prime divisor of \( f(n) \) then

\[
l_{n \to \infty} p_n = \infty.
\]

2.5. *Remark.* We could use much stronger results of Coates [3], who obtained an explicit lower bound for the greatest prime factor of a binary form \( f(x, y) \), irreducible over \( \mathbb{Q} \), however Polya's result is good enough for our purpose.
Proof of Theorem 2.1.

If \( f(1) = 0 \), then by (1.6), \( f(n) = f(n) f(1) \equiv 0 \) for all \( n \). Suppose next that there exists an integer \( k > 1 \) such that \( f(k) = 0 \). We shall show that in this case also \( f(n) \equiv 0 \). By above reasoning it is enough to show that \( f(1) = 0 \). Take any prime \( p > k \). By the Dirichlet's Theorem there exist infinitely many primes \( q \) such that \( (q, k) = 1 \) and \( kq \equiv 1 \) (mod \( p \)). Hence, using (1.6)

\[
0 = f(k) f(q) - f(kq) \equiv f(1) \quad (\text{mod } p),
\]

thus \( f(1) = 0 \).

Assume now that \( f(n) \) never vanishes. From (1.6) it follows that \( f(1) = 1 \).

For a prime \( p \) and a positive integer \( a \), let \( p^r \) be the highest power of \( p \) that divides \( f(p^a) \). Then we write

\[
f(p^a) = mp^r, \quad \text{where } r \geq 0 \text{ and } (m, p) = 1.
\]

Clearly \( m = \pm 1 \), for otherwise if \( q \) is any prime divisor of \( |m| \), then by the Dirichlet's Theorem there exists a prime \( t \), such that \( (t, p) = (t, q) = 1 \) and \( p^a t \equiv 1 \) (mod \( q \)). By virtue of (1.6) we have:

\[
1 = f(1) \equiv f(p^a t) = mp^r f(t) \quad (\text{mod } q)
\]

thus obtaining a contradiction, since \( q \mid m \) and therefore \( mp^r f(t) \equiv 0 \) (mod \( q \)).

Let us now fix prime \( p \). For positive integers \( a, b, a \neq b \) we write:

\[
f(p^a) = m_a p^{r_a}, \quad f(p^b) = m_b p^{r_b},
\]

where \( (p, m_a) = (p, m_b) = 1 \) and \( r_a, r_b \) have the meaning as above. We shall show that \( m_a = m_b \), that is for a fixed prime \( p \) the value of \( m \) in (2.6) is independent of \( a \).

Let \( d = |a - b|, R = |r_a - r_b| \). Since \( p \mid (p^a - p^b) \) than by (2.2) it follows that

\[
f(p^a) = f(p^b) \quad (\text{mod } p).
\]

Using (2.7) and (2.8) we infer that \( r_a \) and \( r_b \) are both zero or both positive. For if one of them were positive and the other equal to zero it would contradict (2.8) in view of \( (p, m_a) = (p, m_b) = 1 \).
Consider first integers $a$ and $b$ for which $|a - b| \neq 2^c$ for any positive integer $c > 0$ and let $|a - b| = d = 2^ce$, where $e$ is odd integer, greater than 1.

Now $p^e - 1$ primitive prime factor $q > 2$. Define

$$L = \begin{cases} p^R m_a - m_b & \text{if } r_a > r_b, \\ m_a - p^R m_b & \text{if } r_a < r_b, \end{cases}$$

then $L \equiv 0 \pmod{q}$. Assuming $m_a \equiv m_b$, we obtain $q \mid p^R + 1$, thus $q \mid p^{2R} - 1$, so $e > 2R$ and since $(e, 2) = 1$, therefore $e \mid R$. It follows now that $q \mid p^R - 1$ so $q \mid 2$ and thus, contradiction shows that $m_a \neq m_b$.

If $|a - b| = 2^c$ for some $c > 0$, then obviously one can find an integer $k$ such that $f(p^k) = m_k p^r k$ and $|a - k| \neq 2^c$, $|b - k| \neq 2^c$. Therefore $m_a = m_k$ and $m_b = m_k$, thus $m_a = m_b$ for all positive integers $a$ and $b$.

We next prove that $m_k = 1$ and $r_k = kr_1$ for all $k > 1$. Keep the prime $p$ fixed. Corresponding to every prime $q \neq p$, there is a prime $t$ such that $(t, p) = (t, q) = 1$ and

$$pt \equiv 1 \pmod{q}. \tag{2.9}$$

In order to show $m_k \equiv 1$, it suffices to prove $m_1 = 1$. Let $f(p^2) = m_2 p^r 2$.

$f(p) = m_1 p^{r_1}$ and $f(pt) = m_1 p^{r_1} f(t)$. By (2.9)

$$m_1^2 p^{2r_1} f^2(t) = f^2(pt) \equiv f^2(1) \equiv 1 \pmod{q}, \tag{2.10}$$

also

$$m_2^2 p^{r_2} f^2(t) = f(p^2)^2 f^2(t) = f(p^2) f(t) f(t) \equiv f(p) f(t) = f(p t) \equiv 1 \pmod{q}. \tag{2.11}$$
Note that \( f(p^2 t) \equiv f(p) \pmod{q} \) since \( f(n) \) is quasi-multiplicative and (2.9) holds. Using (2.10) and (2.11) we obtain that for every prime \( q \neq p \), \( (t,p) = (t,q) = 1 \)

\[
m_2 p^{2 r_2} = m_1^2 p^{2 r_1} \pmod{q}
\]

thus

\[
m_2 p^{r_2} = m_1^2 p^{r_1}.
\]

Since \( m_2 = m_1 \), then \( m_2 = m_1^2 = (\pm 1)^2 = 1 \), so \( m_1 = 1 \) and moreover \( r_2 = 2 r_1 \). We now proceed by induction, and suppose that \( r_n = n r_1 \) for integers \( n < k - 1 \), where \( f(p^n) = p^{r_n} \). For all primes \( q \neq p \) and any prime \( t \) satisfying (2.9) we have:

\[
(2.12) \quad p^{n+1} (f(t))^{n+1} = f(p^{n+1} t) (f(t))^n \pmod{q},
\]

since \( p^{n+1} t \equiv p^n \pmod{q} \), and then \( f(p^{n+1} t) \equiv f(p^n) \pmod{q} \), so (2.12) follows by quasi-multiplicativity.

Using (2.11) we obtain modulo \( q \):

\[
\begin{align*}
p^{n+1} (f(t))^{n+1} & = f(p^{n+1} t) (f(t))^n = f(p^n) (f(t))^n \\
& = p^n (f(t))^n = p^{nr_1} (f(t))^n = (f(pt))^n = f(1) = 1
\end{align*}
\]

and

\[
1 = (f(pt))^{n+1} = p^{(n+1)r_1} (f(t))^{n+1},
\]

thus

\[
p^{n+1} = p^{(n+1)r_1}, \text{ so } r_{n+1} = (n+1)r_1
\]

and by induction \( r_k = kr_1 \) for all \( k \geq 1 \).
To prove the Theorem it only remains to show that if for any two distinct primes \( p \) and \( q \), \( f(p) = p^a \), \( f(q) = q^b \) then \( a = b \). For definiteness assume \( p > q \) and write \( d = |a - b| \) and \( N = p^{d+k}q - 1 > 1 \), where \( k \) is any positive integer. Letting \( x = p^{k/2} \) we consider \( N \) as a polynomial of second degree with respect to \( x \):

\[
N(x) = p^d x^2 q - 1.
\]

It is obvious that \( N(x) \neq a(bx + c)^2 \) and then by Lemma 2.4 the greatest prime factor \( p_n \) of \( N(n) \) goes to infinity with \( n \). Take \( k \) so large that \( N \) has a prime factor \( N_0 > q^d - 1 \). Since \( p^{d+k}q \equiv 1 \pmod{N} \equiv 1 \pmod{N_0} \) then:

\[
p^{a(d+k)}q^b = f(p^{d+k}q) = f(1) \equiv 1 \pmod{N_0}
\]

and

\[
p^{a(d+k)}q^a \equiv 1 \pmod{N_0}
\]

thus

\[
p^{a(d+k)}q^b \equiv p^{a(d+k)}q^a \pmod{N_0}
\]

and therefore \( q^d \equiv 1 \pmod{N_0} \), but \( 0 < q^d - 1 < N_0 \), so \( q^d = 1 \) and \( d = 0 \), proving \( a = b \).

3. FINAL REMARKS

We make the following:

3.1. **Conjecture.** Theorem 2.1 holds even if we assume that a quasi-multiplicative function \( f(n) \) satisfies (2.2) for infinitely many primes \( p \).

We are not able to prove this generalization, however, we shall now show the following:

3.2. **Theorem.** If \( f(n) \) is quasi-multiplicative, integer-valued arithmetic function satisfying (2.2) for infinitely many primes \( p \), then \( f(q^a) = (f(q))^a \) for any prime \( q \) and non-negative integer \( a \).
Proof:

Suppose (2.2) holds for an infinite set of primes \( \beta = \{p_1, p_2, \ldots \} \), and let \( q \) be any prime. We may assume that \( q \not\in \beta \), since otherwise we use (2.2) with the set \( \beta' = \beta - \{q\} \). For any \( p_i \in \beta \) one can find a prime \( t \) such that \( (q, t) = (p_i, t) = 1 \) and \( qt \equiv 1 \pmod{p_i} \). It follows that

\[
\begin{align*}
  f(q) f(t) &\equiv 1 \pmod{p_i}, \\
  q^2 t &\equiv q \pmod{p_i},
\end{align*}
\]

so

\[
\begin{align*}
  f(q^2 t) &= f(q^2) f(t) \equiv f(q) \pmod{p_i}.
\end{align*}
\]

Multiplying (3.4) by \( f(t) \) and using (3.3) we obtain

\[
\begin{align*}
  f(q^2) f^2(t) &\equiv 1 \pmod{p_i}.
\end{align*}
\]

Now \( p^3 t \equiv q^2 \pmod{p_i} \), so

\[
\begin{align*}
  f(q^3 t) &= f(q^2) \pmod{p_i}
\end{align*}
\]

and multiplying (3.6) by \( f^2(t) \) we have:

\[
\begin{align*}
  f(q^3 t) f^2(t) &\equiv 1 \pmod{p_i}
\end{align*}
\]

thus

\[
\begin{align*}
  f(q^3) f^3(t) &\equiv 1 \pmod{p_i}
\end{align*}
\]

by quasi-multiplicativity.

Proceeding further by the same way we infer that for any integer \( n \geq 1 \):

\[
\begin{align*}
  f(q^n) f^n(t) &\equiv 1 \pmod{p_i}.
\end{align*}
\]

From (3.3) it follows that
(3.8) \[ f_n(q) f^n(t) \equiv 1 \pmod{p_i} \]

thus comparing (3.7) and (3.8)

\[ f(q^n) = f^n(q) \pmod{p_i} \]

for infinitely many primes \( p_i \), therefore

\[ f(q^n) = f^n(q). \]

In view of Theorem (3.2), we raise the following:

3.9. Problem. Is it true that if \( f(n) \) is an integer-valued and quasi-multiplicative function that satisfies (2.2) for infinitely many primes \( p \), then \( f(n) \) is multiplicative.

We note that even an affirmative answer to the above problem still leaves Conjecture 3.1. open.

REFERENCES


